Programa para consultar direcciones MAC

Allan Gálvez Fernández, allan.galvez@alumnos.uv.cl

1. Introducción

La modernización y mejora de los sistemas de identificación y autenticación en redes es un tema crucial en el ámbito de la seguridad informática. A medida que el uso de dispositivos móviles y la conectividad en redes Wi-Fi han crecido exponencialmente, la privacidad del usuario se ha convertido en un factor cada vez más relevante. Las direcciones MAC aleatorias (MAC randomization) surgieron como una solución para proteger la privacidad del usuario al evitar el rastreo de dispositivos mediante identificadores únicos de hardware. Este trabajo aborda el diseño e implementación de una herramienta de línea de comandos llamada **OUILookup**, que permite identificar el fabricante de una dirección MAC utilizando APIs públicas de consulta. La importancia de esta herramienta radica en su capacidad de brindar a los administradores de redes y usuarios la posibilidad de identificar dispositivos y analizar la seguridad de sus entornos inalámbricos.

El propósito principal del trabajo es demostrar la factibilidad de utilizar APIs públicas para obtener información de fabricantes a partir de direcciones MAC y cómo esto puede integrarse en flujos de trabajo más amplios de seguridad. La herramienta desarrollada no solo valida el formato de las direcciones MAC, sino que también permite la consulta automatizada y la verificación de dispositivos conectados en la red local, utilizando la tabla ARP. Como principales conclusiones, se identificó que las direcciones MAC aleatorias presentan desafíos adicionales para la autenticación en redes corporativas y soluciones basadas en listas de control de acceso (ACLs), destacando la necesidad de enfoques más integrales como la autenticación basada en certificados.

2. Descripción del problema y diseño de la solución

El problema principal que aborda este trabajo es la identificación de fabricantes a partir de direcciones MAC en redes que pueden estar utilizando aleatorización de direcciones. La aleatorización de direcciones MAC complica la administración y seguridad de redes empresariales, ya que las direcciones cambian con frecuencia, impidiendo la autenticación y rastreo de dispositivos. Además, en entornos donde las direcciones MAC se utilizan para autorizar dispositivos (por ejemplo, en portales cautivos), la aleatorización interfiere con las listas de control de acceso y las soluciones de seguridad basadas en el filtrado de direcciones.

Requerimientos y especificaciones:

•Crear una herramienta basada en línea de comandos que permita:

1. Validar el formato de las direcciones MAC ingresadas por el usuario.
2. Consultar el nombre del fabricante usando una API REST pública.
3. Mostrar la lista de dispositivos conectados a la red local mediante la tabla ARP.

• La herramienta debe procesar los argumentos ingresados y retornar resultados en tiempo real.
• La consulta a la API debe manejar correctamente errores de conexión y direcciones no encontradas.

Diseño de la Solución

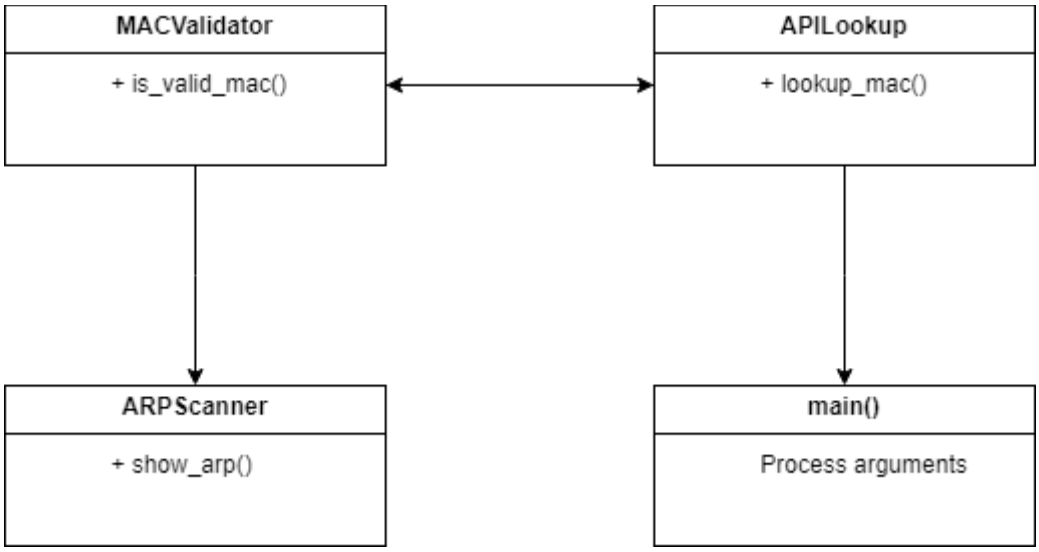
El diseño general de la herramienta se organiza en dos módulos principales:

1. **Módulo de validación**: Verifica el formato de la dirección MAC ingresada.
2. **Módulo de consulta**: Realiza la solicitud HTTP a la API y analiza la respuesta para extraer la información del fabricante.

3. Modelo General de Arquitectura

La solución se estructura en tres clases principales:

1. Clase MACValidator: Implementa los métodos para validar direcciones MAC.
2. Clase APILookup: Gestiona las solicitudes y respuestas de la API de consulta.
3. Clase ARPScanner: Ejecuta comandos del sistema para mostrar la tabla ARP y extrae las direcciones MAC.



4. Implementación

Durante la implementación de la herramienta, se desarrollaron tres clases principales, cada una con una funcionalidad específica:

1. **Clase**

MACValidator:

Se implementó utilizando expresiones regulares para validar el formato de direcciones MAC. Los principales desafíos encontrados fueron la compatibilidad de diferentes formatos, como aa:bb:cc o aa-bb-cc, que tuvieron que ser cubiertos con diferentes patrones de expresión regular.

2. **Clase**

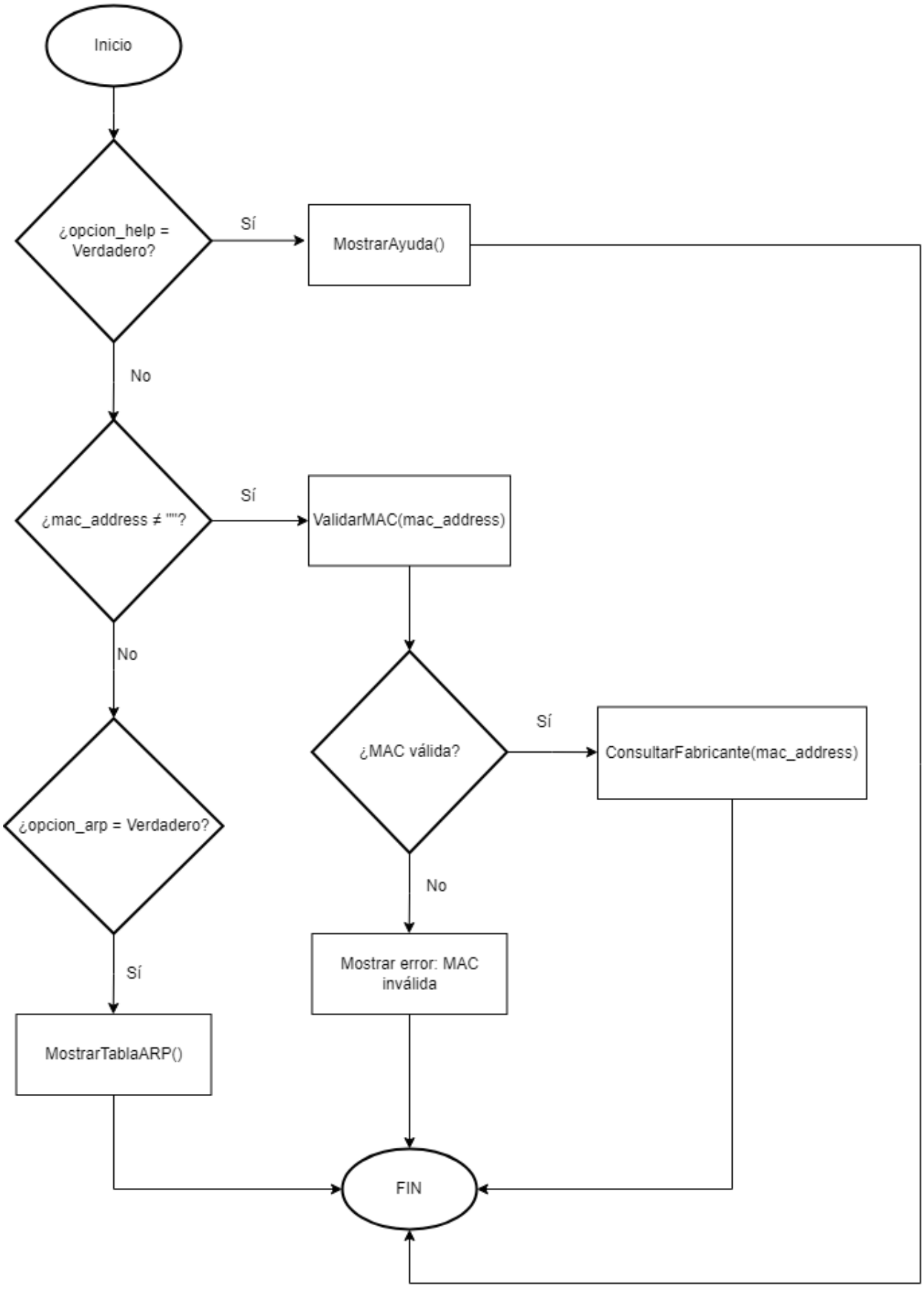
APILookup:

Esta clase se encarga de realizar las solicitudes a la API REST para consultar fabricantes. Se implementaron manejadores de errores para gestionar respuestas HTTP no exitosas y tiempos de espera en la conexión. Se utilizó la librería requests de Python, que permitió simplificar la comunicación con la API y el manejo de datos JSON.

3. **Clase**

ARPScanner

Utiliza el comando arp -a para extraer las direcciones MAC de dispositivos conectados en la red local. El principal reto fue manejar el procesamiento de la salida del comando arp, que varía dependiendo del sistema operativo. Se implementaron métodos adicionales para adaptar la salida a formatos específicos de direcciones MAC.


Inicio
¿opcion_help = Verdadero?
Sí
MostrarAyuda()
No
¿mac_address ≠ ""?
Sí
ValidarMAC(mac_address)
No
¿MAC válida?
Sí
ConsultarFabricante(mac_address)
No
Mostrar error: MAC inválida
¿opcion_arp = Verdadero?
Sí
MostrarTablaARP()
FIN

Funcionamiento de las direcciones MAC aleatorias en dispositivos electrónicos

Las direcciones MAC (Media Access Control) son identificadores únicos asignados a las tarjetas de red de dispositivos como computadoras, teléfonos y routers. Originalmente, estas direcciones eran fijas, lo que permitía a los administradores de red y a terceros rastrear los dispositivos en redes locales y públicas. La aleatorización de direcciones MAC surge como una medida de seguridad para proteger la privacidad de los usuarios al evitar que su dispositivo sea identificado a través de la red a la que se conecta. Esta técnica consiste en generar direcciones temporales y dinámicas que reemplazan la dirección MAC original del dispositivo durante la búsqueda de redes o al conectarse a redes desconocidas.

Funcionamiento

1. Generación de Direcciones Aleatorias: Cuando un dispositivo busca redes Wi-Fi cercanas, utiliza direcciones MAC aleatorias en lugar de su dirección real para evitar ser rastreado. Esta funcionalidad está implementada en dispositivos modernos como iPhones a partir de iOS 8 y en dispositivos Android desde la versión 6.0.
2. Cambio de Direcciones: Cada vez que el dispositivo se conecta a una nueva red o realiza un escaneo, se genera una nueva dirección MAC temporal, evitando que las redes puedan registrar un patrón de conexiones asociado al usuario.
3. Uso de Direcciones Originales: Una vez que el dispositivo se conecta a una red conocida o segura (como la red doméstica), utiliza su dirección MAC original para realizar la autenticación y garantizar una conexión estable.

Desafíos e Impacto

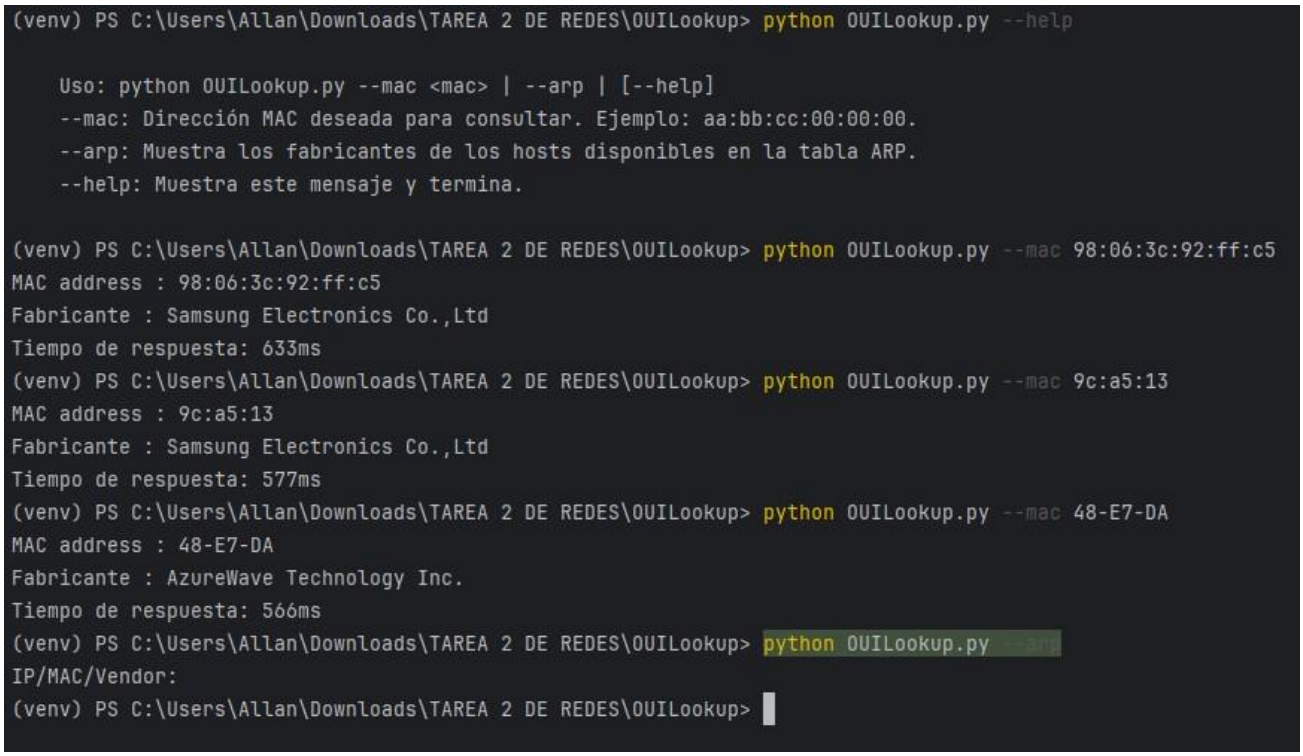
Aunque la aleatorización de direcciones MAC protege la privacidad del usuario, presenta desafíos en redes empresariales y otros entornos que dependen de la autenticación basada en MAC. Los administradores de red deben actualizar constantemente sus listas de control de acceso (ACL) para permitir la conexión de dispositivos autorizados. Además, esta técnica puede interferir con sistemas de monitoreo que dependen de direcciones MAC fijas para identificar y gestionar dispositivos en la red.

Sección Referencias.[1] [2] [3].

5. Pruebas

Para garantizar el funcionamiento correcto del script OUILookup.py, se llevaron a cabo una serie de pruebas que cubren todos los casos de uso posibles, incluyendo validación de entradas, manejo de errores y consultas a la API. Estas pruebas se diseñaron para asegurar que cada funcionalidad del script se ejecute correctamente en distintos escenarios y que los resultados sean coherentes con las expectativas definidas.

Se validaron diferentes formatos de direcciones MAC para asegurar que el script acepte solo entradas en formatos correctos y maneje los errores adecuadamente. La función is_valid_mac() fue probada con las siguientes entradas:



6. Conclusión

El desarrollo de la herramienta OUILookup permitió la implementación de una aplicación funcional para consultar el fabricante de una dirección MAC y mostrar las direcciones MAC. La herramienta fue capaz de identificar correctamente los fabricantes de las direcciones MAC proporcionadas registradas en la base de datos de la API detectando las siguientes macs:

mac 98:06:3c:92:ff:c5

mac 9c:a5:13

mac 48-E7-DA

Durante el desarrollo de OUILookup, se adquirió experiencia en el uso de APIs REST para realizar solicitudes y procesar respuestas de manera eficiente utilizando la librería requests. Además, el uso de expresiones regulares para validar direcciones MAC resultó ser una técnica versátil y precisa que podría aplicarse a otros escenarios de validación de datos. También se destacó la importancia de automatizar tareas como la revisión de la tabla ARP, lo que facilita el monitoreo de dispositivos en redes locales.

Limitaciones Encontradas

Aunque se logró procesar direcciones MAC en los formatos estándar, el soporte para formatos menos comunes no se implementó, lo que limita su aplicabilidad en ciertos entornos de red. Otro aspecto que no se alcanzó fue la compatibilidad multiplataforma completa, ya que el uso de comandos específicos para cada sistema operativo (como arp -a en Windows y arp en Linux) generó problemas en algunos entornos.

Posibles Mejoras

- **Optimizar el uso de la API** creando un sistema de caché para almacenar los resultados de fabricantes consultados previamente, mejorando así la velocidad del programa.
- **Compatibilidad multiplataforma**: Se podría integrar el uso de librerías como scapy o netifaces para manejar la extracción de la tabla ARP de forma homogénea en diferentes sistemas.
- **Soporte para más formatos de MAC**, ampliando las expresiones regulares para reconocer direcciones con variaciones.
- **Agregar autenticación a la API** en caso de utilizar servicios con credenciales, lo que abriría la posibilidad de trabajar con fuentes de datos más completas y precisas.
- **Función de exportación** para generar informes en CSV o JSON y facilitar el análisis de dispositivos consultados.

Estas mejoras no solo harían que la herramienta sea más robusta, sino que la harían más flexible y fácil de adaptar a diferentes necesidades y entornos de red.

7. Referencias

[1] Tanenbaum, A. S. y Wetherall, D. J. (2012). *Redes de computadoras*. Pearson Educación. https://bibliotecavirtualapure.wordpress.com/wp-content/uploads/2015/06/redes_de_computadoras-freelibros-org.pdf

[2] Estrada, A. (2016). *Seguridad en Redes*. DarFE Learning Consulting, S.L. https://elhacker.info/manuales/Libros%20hack/seguridadenredes.pdf

[3] Fernández, L. (17 de septiembre de 2024). *Qué es la dirección MAC, cómo cambiarla y riesgos del filtrado MAC.* Redeszone. https://www.redeszone.net/tutoriales/redes-cable/direccion-mac-que-es-como-cambiarla